A Comparative Study of the Method of CRT and a Method Discovered by the Author to Solve a Class of Standard Quadratic Congruence of Composite Modulus-a Product of Two Primes

Prof. B M Roy
Head, department of mathematics
Jagat arts, commerce & i h p science college, goregaon
Dist: gondia, maharastra (india) pin: 441801
(affiliated to r t m nagpur university, nagpur)

Abstract

In this paper, finding solutions of a class of solvable standard quadratic congruence of composite modulus using CRT is compared with the method (formulation) discovered by the author. Formula is tested true by solving suitable examples. The author's method of solving standard quadratic congruence is found very simple, short and time-saving in comparison to the method found in the literature of mathematics $i.e.$ using Chinese Remainder Theorem (CRT). A comparative study of the two methods is made. No need to use CRT.

Key-Words: *Chinese Remainder Theorem, composite modulus, Formulation.*

I. INTRODUCTION

Many standard quadratic congruence of composite modulus have been formulated by me and it is found that the formulation made the finding of the solutions easy and time-saving. The students / readers find the formulation a very quick method for solutions.

Here in this paper, the existed method (Use of CRT) and method discovered by the author are compared solving two different standard quadratic congruence of composite modulus:

$$x^2 \equiv a^2 (mod\ pq), where\ p, q\ are\ odd\ positive\ prime\ integers;\ p, q\ may\ be\ twin\ prime.$$

II. LITERATURE REVIEW

Many books on Number Theory is referred but find no formulation for the congruence under consideration. They used the Chinese Remainder Theorem [1] for the solutions. It is not a fair method for students / readers. Thomas Koshy had attempted solving these congruence of composite modulus [2] but using CRT.

It seems that no one cared for it. No one was interested to solve the problem by formulation. All were busy to consider the standard quadratic congruence of prime modulus. This pained me very much.

III. NEED OF RESEARCH

The use of Chinese Remainder Theorem is a long and time-consuming method. Students find themselves in a dilemma. They always remain in search of a new suitable and easy method to find all the solutions quickly. Formulation is the only remedy for them. I tried my best to formulate the solutions of the congruence. I want to compare the two methods. This is the need of my research.

IV. PROBLEM STATEMENT

Here, in this paper, my aim is to compare the method of CRT and the method discovered by formulation of the problem: $x^2 \equiv a^2 (\ mod\ pq\ )$, where p, q are odd positive prime integers; may be twin primes.

V. EXISTED (OLD) METHOD OF SOLUTION

Consider the congruence $x^2 \equiv a^2 (mod\ pq)$.

It is always solvable and has exactly four solutions [4].

The said congruence can be solved by Chinese Remainder Theorem as below.

It can be split into two in the form: $x^2 \equiv a^2\ (mod\ p)$; $x^2 \equiv a^2\ (mod\ q)$.

Both the congruence have two-two solutions such as say:

$$x \equiv x_1, x_2\ (mod\ p); \quad x \equiv x_3, x_4\ (mod\ q).$$

Then the four common solutions are given by Chinese Remainder Theorem.

$$x_0 \equiv k, l,\ m,\ n\ \ (mod\ pq).$$

Sometimes it is found in the form $x^2 \equiv b\ (mod\ pq)$.

It can be written as $x^2 \equiv b + k.p = a^2\ (mod\ pq)$[2]. Then we can proceed as above.

VI. ILLUSTRATIONS

Consider the congruence $x^2 \equiv 23\ (\text{mod } 77)$. Here, $77 = 7.11$ giving $p = 11, q = 7$.

It can be written as $x^2 \equiv 23 \equiv 2\ (\text{mod } 7)$ & $x^2 \equiv 23 \equiv 1\ (\text{mod } 11)$

The corresponding solutions are $x \equiv 3, 4\ (\text{mod } 7)$ &

$x \equiv 1, 10\ (\text{mod } 11)$ HOW?

Now CRT can be used to find all the four common solutions:

Consider $x \equiv 3, 4\ (\text{mod } 7)$ & $x \equiv 1, 10\ (\text{mod } 11)$

Here $a_1 = 3,\ 4$; $a_2 = 1,\ 10$; $m_1 = 7$; $m_2 = 11$.

Then, $(m_1, m_2) = (7,\ 11) = 1$. $M = m_1.m_2 = 7.11 = 77$.

$M_1 = \frac{M}{m_1} = \frac{77}{7} = 11$; $M_2 = \frac{M}{m_2} = \frac{77}{11} = 7$.

Then consider the congruence $M_1 x \equiv 1\ (\text{mod } m_1)$

i. e. $11x \equiv 1\ (\text{mod } 7)$ i. e. $x \equiv 2\ (\text{mod } 7)$ i. e. $x_1 = 2$. How?

Also consider the congruence $M_2 x \equiv 1\ (\text{mod } m_2)$

i. e. $7x \equiv 1\ (\text{mod } 11)$ i. e. $x \equiv 8\ (\text{mod } 7)$ i. e. $x_2 = 8$. How?

The common solutions by CRT are $z_0 \equiv a_1 M_1 x_1 + a_2 M_2 x_2 \equiv 10, 67, 32, 45\ (\text{mod } 77)$.

[Tabular calculations are not shown]

VII. AUTHOR'S METHOD (by Formulations)

Let us now consider the congruence under consideration $x^2 \equiv a^2\ (\text{mod } pq)$,

where p, q are odd positive prime integers. Such type of congruence is always solvable

and has exactly four solutions [4] .

Two obvious solutions are $x \equiv \pm a \pmod{pq} \equiv a,\ pq - a \pmod{pq}$.

For the other two solutions, consider $x \equiv \pm(pk \pm a) \pmod{pq}$.

Then $x^2 = (pk \pm a)^2 = a^2 + p.qm$, if $k.(pk \pm 2a) = qm$.

i. e. $x^2 \equiv a^2 \pmod{pq}$ is satisfied.

If $pk \pm 2a = qm$, then other two solutions are $x \equiv \pm(pk \pm a) \pmod{pq}$.

But if it happens that p & q are twin primes, then $q = p - 2$.

Then for $x = \pm(p-1)a$, we see that $x^2 \equiv a^2 \pmod{pq}$ is also satisfied.

Thus two other solutions are $x = \pm(p-1)a \pmod{pq}$.

VIII. ILLUSTRATIONS

Now we solve same congruence solved above using the discovered formulae.

Consider the congruence $x^2 \equiv 23 \pmod{77}$ with $77 = 7.11$ $p = 11, q = 7$.

It can be written as $x^2 \equiv 23 + 77 = 100 = 10^2 \pmod{77}$.

Its two obvious solutions are $x \equiv \pm 10 = 10; 67 \pmod{77}$.

For other two solutions, $pk \pm 2a = 11.2 \pm 2.10 = 22 \pm 20 = 42 = 7.6 = 6q$.

So, other two solutions are: $x \equiv \pm(pk \pm a) \pmod{77}$ i. e. $x \equiv \pm(11.2 \pm 10) \pmod{77}$.

$x \equiv \pm 32 \pmod{77}$ i. e. $x \equiv 32, 45 \pmod{77}$.

It is seen how easily the solutions are obtained!!

Thus the required solutions are $x \equiv 10, 67; 32, 45 \pmod{77}$ same as obtained above by heavy and boring calculations.

Sometimes we can have the congruence $x^2 \equiv 36 \pmod{1763}$.

Here, $1763 = 41.43$ with $p = 43, q = 41$; p, q are twin primes.

Two obvious solutions are $x \equiv \pm 6 \pmod{1763}$ i. e. $x \equiv 6, 1757 \pmod{1763}$.

The other two solutions are $x \equiv \pm(p-1)a \pmod{pq}$ i. e. $x \equiv \pm 252 \pmod{1763}$.

i. e. $x \equiv 252, 1511 \pmod{1763}$.

Thus, the all the solutions are $x \equiv 6, 1763;\ 252, 1511 \pmod{1763}$.

Using CRT, we have to spare at least 30 minutes but formulation gives all the solutions within a minute!!

Let us consider some more examples: [1] $x^2 \equiv 25\ (mod\ 7743)\ \ with\ \ 87.89 = 7743; p = 89, q = 87.$

[2] $x^2 \equiv 9\ (mod\ 3363)\ \ with\ \ 57.59 = 3363; p = 59, q = 57.$

IX. CONCLUSION

Thus it can be concluded that we need not use CRT for solutions of solvable standard quadratic congruence of composite modulus. It saves time of calculation. It is easier than the use of CRT.

X. MERIT OF THE PAPER

The congruence under consideration is formulated and are compared successfully. First time the formulation is used for solutions. It saves time in calculation. Formulation is the merit of the paper.

REFERENCE

[1] Burton David M, Elementary Number Theory, Seventh Indian edition, Mc Graw Hill (Pvt) Ltd.
[2] Koshy Thomas, Elementary Number Theory with Applications, second edition, Indian Print, 2009.
[3] Roy B M , Discrete Mathematics & Number Theory, First edition, Das Ganu Prakashan, Nagpur (INDIA)
[4] Zuckerman at el, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, 2008.